DEPARTMENT OF THE NAVY
USMC, USN, DON
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

4 March 2022

JOINT MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF NAVY RISK MANAGEMENT FRAMEWORK RECIPROCITY

Ref: (a) Department of Defense Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 28 July 17, change 3, 29 Dec 20
(b) Department of Defense Instruction (DoDI) 8531.0, DoD Vulnerability Management, 15 Sep 20
(c) Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, 14 Mar 14, change 1, 7 Oct 19
(d) Department of Defense Instruction (DoDI) 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, 7 Mar 2016, change 1 of 25 Jul 17
(e) Department of Defense Cloud Computing Security Requirements Guide, v1.0 r4,14 Jan 22
(f) CNSSI 1254, Committee on National Security Systems Instruction, Aug 2016

1. This policy is consistent with and supports references (a) through (f) and is effective upon release. It applies to all systems and all Authorizing Officials (AOs) and Security Control Assessors (SCAs), whether the Service is the deploying or receiving component.

2. The purpose of this policy is to advance cybersecurity reciprocity in the Department of Navy (DON) and reduce duplicative testing, assessment, documentation to increase data driven risk-informed decisions and support digital modernization efforts.

3. The following guidelines are to be applied as the basis for practicing reciprocity in accordance with reference (a).

a. The default option is for Services to use each system/application in its native environment. This use case will be referred to as “co-use” and will only require authorization by the deploying component.

(1) Deploying components are responsible for establishing notification processes (e.g. cybersecurity incidents, PII breaches, etc) for co-use systems, applications, and cloud services.

(2) The Cyber Security Service Provider (CSSP) providing support to the co-use systems, applications, and cloud services is responsible for protecting the Naval data contained therein. Additional coverage by another CSSP is prohibited.

b. When an authorized, operational system and/or application in one environment is designated for install and use in another environment, cybersecurity reciprocity will be the default method for assessment and authorization by the receiving component.

(1) Prior to initiating testing or a risk assessment for a system to be hosted in the receiving component's environment, the receiving AO is responsible for determining whether the system has been authorized by another AO.

(a) If current authorization exists, the receiving AO and SCA will proceed with reciprocity based on RMF documentation required by reference (a).

(2) When the specific documents required by reference (a) are not available, the receiving AO must consider the body of technical evidence available from the Program Office or system owner, to include, but not limited to the following information:

(a) List of vulnerabilities with residual risk
(b) Residual risk assessment for each Very High or High risk vulnerability
(c) Defense-in-depth security architecture for the platform (building, ship, Humvee, command center, etc.) and enclave
(d) Interface diagrams and cross-domain interfaces that specify type of interface, direction of data flow, and any in-line security solutions
(e) Impact and technical justification for any Very High or High risk vulnerabilities that remain
(f) Vulnerability management and incident management plans

(3) Requests for documentation not included in the deploying component's RMF package must be endorsed by the requesting Service CISO before being forwarded to the deploying AO.

(4) The deploying AO will ensure documentation providing the body of technical evidence is freely shared with the receiving component.

(5) The receiving component becomes responsible for establishing and maintaining a full authorization if it continues using any system, application, or cloud service that is no longer supported by the deploying component.

c. Denials to support reciprocity will be escalated through respective service chains of command to the appropriate Deputy DON Senior Information Security Officer as required to resolve in a timely manner.

SPINKS.RENATA.CHARECE.1244803594
Digitally signed by SPINKS.RENATA.CHARECE.1244803594
Date: 2022.03.04 14:52:48 -05'00'

Renata Spinks
US Marine Corp
Senior Information
Security Officer

BRYERJOYNER.SUSAN.1066201534
Digitally signed by BRYERJOYNER.SUSAN.1066201534
Date: 2022.03.04 17:42:28 -05'00'

RDML Susan BryerJoyner
US Navy
Senior Information
Security Officer

PLATER.ALVIN.A.1042145145
Digitally signed by PLATER.ALVIN.A.1042145145
Date: 2022.03.04 09:37:14 -05'00'

Tony Plater
Department of the Navy
Chief Information
Security Officer

Distribution:
VCNO
ACMC
ASN (RD&A)
ASN (M&RA)
ASN (EI&E)
ASN (FM&C)
DUSN (P)
OCMO
NCIS
CNR
CHINFO
DON/AA
DASN (RDT&E)
DASN (M&B)
DASN (E&LM)
DASN (C4I & SPACE)
DASN (AP)
DASN (UxS)
DNS
DMCS
OPNAV (N1/N2N6/N3/N5/N4/N8/N9)
HQMC (DCI)
HQMC (IC4)
HQMC (DC P&R)
HQMC (DC, PP&O)
DON Deputy CIO (Navy)
DON Deputy CIO (Marine Corps)
FLTCYBERCOM/10THFLT
COMNAVAIRSYSCOM
COMNAVSEASYSCOM
COMNAVWARSYSCOM
COMNAVSUPSYSCOM
COMNAVRESFORCOM
COMNAVSPECWARCOM
COMNAVFACENGCOM
COMUSFLTFORCOM
COMMARFORCOM
COMPACFLT
COMUSNAVEUR/AF/C6F
COMUSNAVCENTCOM
COMNAVSO
COMOPTEVFOR
PEO DIGITAL
PEO C4I
PEO MLB

Distribution (con’t):
MARCORSYSCOM
MARFORCYBER
MARCORLOGCOM
MCICOM
TECOM
MCRC
MCCS
MARFOREUR
MARFORPAC
MCIA
MCCDC
MCTSSA
MARFORRES
MARFORCOM
MARFORSOC
MARFORCENT
MCCOG
ONR
ONI
NRL
NIA
CNIC
BUMED
BUPERS
DIRSSP
COMNAVDIST
COMNAVSAFECEN
USNA
FLDSUPPACT
NAVHISTHERITAGECOM
NETC
NAVPGSCOL
NAVWARCOL